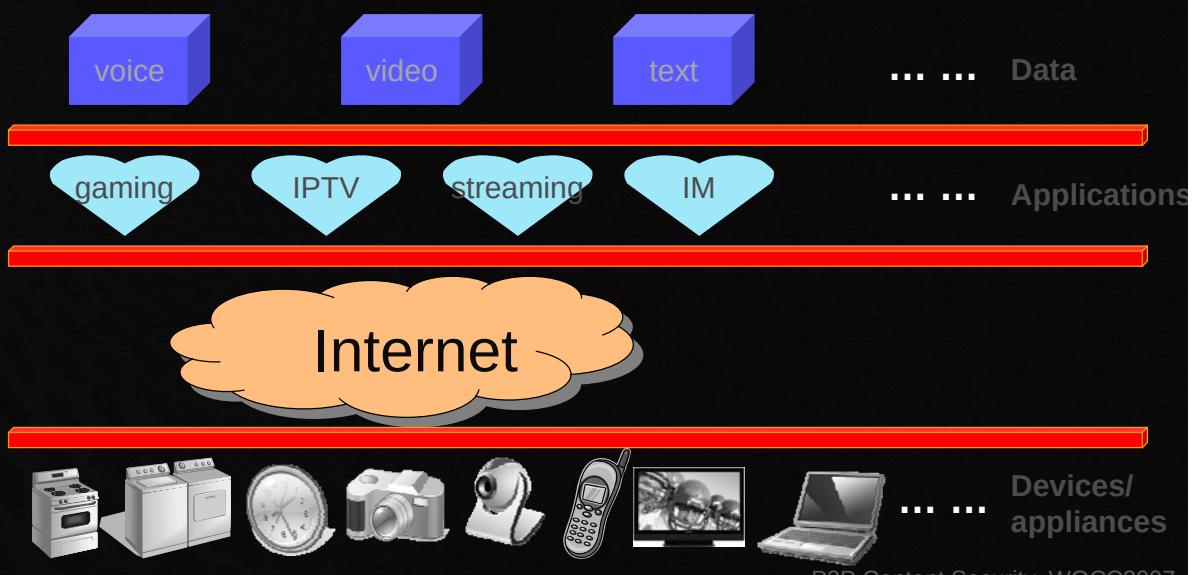
Why Jenny can't share the content with Jane?

- Content Security in P2P

Heather Yu
Huawei Technologies
heathery@ieee.org

Future of Networked Home

- A vision



The World of Content Sharing

- Napster made its debut in 1999
- P2P content sharing became immensely popular
  - 200million users downloading sw using KaZaA
  - >5million BitTorrent population
  - ~ 10million Gnutella, FastTrack, eDonkey
  - 50%-75% Internet traffic

Skype

- Oct. 2006
  - 135,900,000 world wide
  - 21,744,000 in US
  - Total revenue $50million in last quarter of 2006
  - 6.6 billion skype-to-skype minutes
  - 1.1 billion skype-out minutes

P2P Overlay Multicast and Streaming

- PPLive
  - 12/2004, created at Huazhong Univ. of Science and Tech., China
  - “P2P television network”
  - Largest live multimedia streaming system in the world
  - 12/2005, 20million downloads
  - 400,000 aggregated users/day
  - 1 overlay/channel; 400+ channels; thousands of peers/channel at peek
  - 200,000 peers at Chinese New Year2006

Why Is It So Popular

- “Free” content
- Opportunity for high availability and scalability
  - Provide user ability to locate and obtain a wide variety of content
- *Fueled academic research*

What's Against P2P

- Low and asymmetric bandwidth
  - ADSL - 1.4Mbps down, 400Kbps up
  - Cable modems - 1.5-3Mbps down, 400-600Kbps up
- Best effort service insufficient for most applications
- Lack of interoperability

- Law suits against service provider and users
- Lack of trust, security, DRM mechanisms

Skype

- Hybrid
  - Supernode & ordinary node

- Privacy
  - Specify privacy level – only allow calls from contact list
- Virus, worm, spyware, fishing, ……
  - No protection
- Firewalls
  - Allow calls to go through firewall
- Skype central server issue Digital Certificate based on user name and password
  - Establish identity
- Skype messages encrypted end-to-end

Content security is not just a technology problem

Lawsuit, lawsuit, lawsuit

Outline

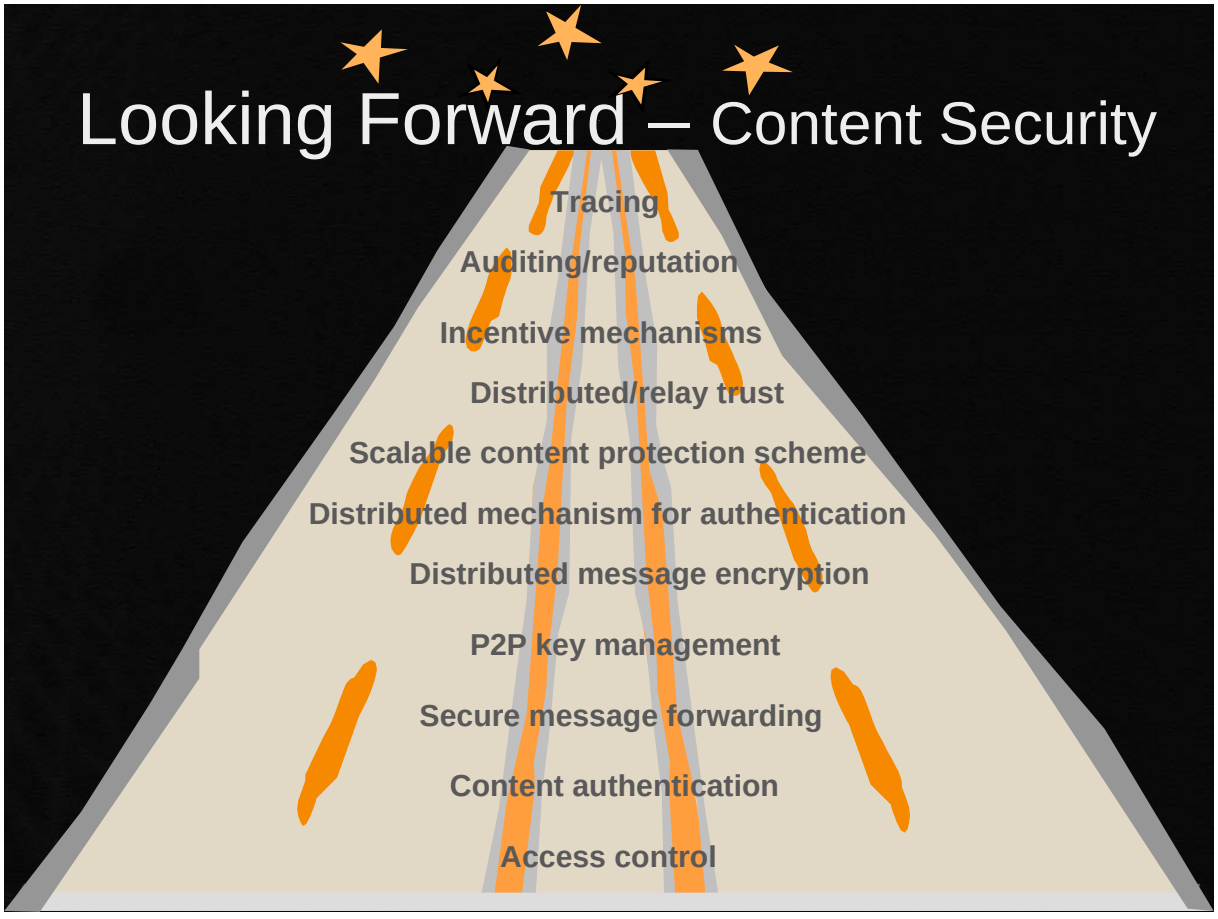
- P2P Content Security Open Problems
- P2P Content Security in OM
- How to Win the Game in the P2P War

P2P Content Security

Security – a Barrier to P2P Adoption

- The downside
  - Distributed in nature, wide availability of replicated objects
  - Exposed to network poison, distributed viruses worms, Trojan horses, or spyware
  - Existing client-server based security tech. does not apply to p2p
  - Hard to make those with different security systems on different platforms and etc. to interoperate
  - When go through firewall to public net, security and privacy issues go up several orders of magnitude
  - Fairness issues in resource sharing
  - 'Free' content distribution, 'free' malicious/fake content
  - Hijacking of queries, denial of service
  - Trust and privacy issues
  - ……

Looking Forward – Content Security



The Hopeful

- The upside
  - information is distributed
    - no convenient point of attack for intruders
  - Smaller damage of DoS attack

P2P Content Security in OM - Secure Message Forwarding

Attacks and Anti-attacks

- Goals of Attacks
  - Stole data/false data forwarding
  - Traffic analysis
  - Resource abuse/manipulation by selfish peer
- Network → overlay → application layer
  - Secure overlay routing
  - Best-effort service → malicious peers many opp. to corrupt content/P2P communications at overlay
    - Sybil attack, node ID attack, routing table attacks, DoS, overlay partition attacks, data placement attack, **message forwarding attack**, traffic analysis, unmerited resource sharing … – overlay level attack
  - Ensure integrity and authenticity of data
    - Network poisoning, returning false data to query … … – application level attack

Stole Content via NodeID Attack

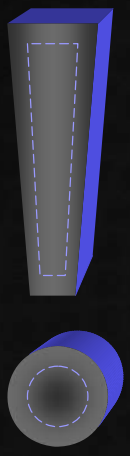
- To obtain a specific nodeID
  - Max probability to be closer to an object/content
  - Mediate victim's access to content/censor content object
- Straightforward anti-attack mechanism
  - Centralized certificate authority
  - ? How to assign random nodeIDs securely w/o centralized authority

False Content via Message Forwarding Attacks

- Attacks
  - Network poison
  - Query hijacking
  - Message hijacking
  - On the road message swapping
- Secure message forwarding
  - Ensure at least one copy of a message sent to a key(peer) reaches the correct peer with high probability

Secure Message Forwarding

- Previous art
  - Failure testing
  - Replicated messaging through multiple routes
  - Random route
  - Real time constraint, cost



P2P will play a key role in next-gen networks & business applications

How can we make it possible for Jenny to share the content w/ Jane in a way that is easy and convenient

Protect content w/o hijacking user convenience

– Jenney will be able to share the content w/ Jane!

The Possibilities, Diff. Approach?

- Can security be improved by … … ?

- Can we … … ?

THANK YOU

heathery@ieee.org